

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

L'usage de signatures électroniques dans le cadre du Règlement eIDAS

Losdyck, Bénédicte

Published in:

L'identification électronique et les services de confiance depuis le règlement eIDAS

Publication date:

2016

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Losdyck, B 2016, L'usage de signatures électroniques dans le cadre du Règlement eIDAS. Dans *L'identification électronique et les services de confiance depuis le règlement eIDAS*. Collection du CRIDS, Numéro 39, Larcier , Bruxelles, p. 139-137.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

L'usage de signatures électroniques dans le cadre du Règlement eIDAS

Bénédicte Losdyck*

Introduction

1.- Mise en contexte. Cette contribution s'inscrivant dans le cadre d'un ouvrage consacré au Règlement eIDAS dans sa globalité, il est naturellement impossible de parcourir l'ensemble du corpus législatif applicable par ailleurs à la signature électronique. D'excellentes études sur la question auxquelles chacun peut se reporter ont déjà été publiées¹. Par ailleurs, une série de questions a volontairement été laissée de côté dans la mesure où ces questions sont traitées dans les autres contributions du présent ouvrage. L'objectif de la présente contribution est précisément de faire le point sur les nouveautés qu'apporte le Règlement eIDAS² au régime légal applicable aux signatures électroniques.

2.- Formalités *ad probationem* et *ad validitatem*. Avant d'entamer notre analyse, nous attirons l'attention du lecteur sur le fait qu'en terme de preuve les questions relatives à la validité des signatures, qu'elles

* Bénédicte Losdyck est chercheuse au CRIDS et travaille actuellement sur le projet *Hybrid Electronic Curation and Transformation of Records*. Elle est également avocate au barreau de Bruxelles. Cette contribution doit beaucoup à Jean-Benoît Hubin, Hervé Jacquemin et Johan Vandendriessche avec qui nous avons eu d'intéressants échanges. Qu'ils en soient remerciés.

¹ D. GOBERT, « Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001 », in *La preuve*, Liège, Formation permanente CUP, vol. 54, 2002, pp. 83-172 ; E. MONTERO et H. JACQUEMIN, « Commerce électronique et contrats de l'informatique », *Chronique de jurisprudence en droit des technologies de l'information (2009-2011)*, R.D.T.I., 2012/48-49, pp. 5-28 ; P. VAN EECHE, « De elektronische handtekening in het recht », R.D.C., 2009, pp. 323-354 ; D. MOUGENOT, « La preuve et les nouvelles technologies », *La preuve au carrefour de cinq disciplines juridiques* Limal, Anthemis, 2013, pp. 161 et s. ; J. VANDENDRIESSCHE, « De elektronische handtekening », in R. DE CORTE (ed.), *Praktijkboek Recht en Internet*, Bruges, Vanden Broele, 2013, pp. 1-56.

² Règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, J.O.U.E., L. 257/73 du 28 août 2014.

soient manuscrites ou électroniques, ne sont généralement soulevées que lorsque celles-ci font l'objet d'une contestation. En pratique, ces questions sont souvent ignorées, bien qu'elles aient récemment connu de nouvelles applications suite à l'usage de plus en plus fréquent de la signature dans l'environnement numérique. En outre, sous réserve de certaines exceptions, les parties sont libres de convenir des règles qui s'appliqueront dans leur relation en matière de preuve, et plus particulièrement, en matière de signature électronique. En effet, en vertu du droit commun des obligations, les dispositions ayant trait à la signature ne sont, dans la plupart des cas, ni impératives, ni d'ordre public.

Néanmoins, dans certaines hypothèses, le législateur belge considère la signature comme une condition de validité de l'acte. Dans de tels cas, l'absence de signature pourrait affecter la validité de l'acte. Par exemple, les contrats de crédit à la consommation doivent, sous peine de sanction, nécessairement être conclus au moyen d'une signature manuscrite ou d'une signature électronique qualifiée³.

Lorsque des cocontractants veulent se ménager la preuve qu'un contrat a valablement été conclu, qu'une administration souhaite signer électroniquement des documents ou qu'un citoyen veut soumettre sa déclaration d'impôt via *Tax on Web* par exemple, il est primordial que la signature apposée soit fiable. L'environnement dématérialisé, dans lequel se nouent désormais de plus en plus fréquemment les relations juridiques, soulève donc la question de la possibilité de recourir à une signature électronique pour se ménager une preuve de son droit ou respecter une formalité exigée *ad validitatem*. En fonction des circonstances et des risques inhérents à celles-ci, il convient de déterminer quel procédé de signature doit être utilisé pour signer valablement dans l'environnement numérique.

3.- Plan de la contribution. Le premier chapitre de cette contribution décrit brièvement les dispositions légales qui régissent actuellement l'usage de la signature électronique en droit belge. Le second chapitre détaille quant à lui le nouveau régime juridique qui entrera en vigueur suite à l'adoption du Règlement européen eIDAS et les changements apportés par cette nouvelle réglementation.

³ Art. VII. 78 CDE. Pour de plus amples développements à ce sujet, voy. la contribution de H. Jacquemin dans le présent ouvrage.

CHAPITRE I. Le cadre légal antérieur entourant l'utilisation des signatures électroniques

SECTION 1. – La directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques

4.- Ratio legis de la directive. Dès 1997, une communication visant à assurer la sécurité et la confiance dans la communication électronique fut émise par la Commission européenne. Celle-ci révèle les premières préoccupations de la Commission concernant la signature électronique⁴. Cette communication fut rapidement suivie par l'adoption en décembre 1999 d'une directive sur un cadre communautaire pour les signatures électroniques⁵.

L'utilisation de plus en plus fréquente d'internet pour nouer des relations contractuelles nécessitait que le régime probatoire de l'acte sous seing privé soit remanié. En effet, aussi bien les commerçants que les particuliers commençaient à s'engager contractuellement à distance sans qu'aucun contrat ne soit signé de manière manuscrite. Or, fondé sur une conception formaliste des notions d'écrit et de signature, ce régime n'était plus en phase avec les nouvelles possibilités qu'offre le réseau⁶. Au risque d'exclure ces contrats dématérialisés du domaine de la preuve littérale, il était primordial de déterminer les conditions de recevabilité et la valeur probante de tels documents⁷.

La directive 1999/93/CE avait donc pour objectif d'assurer une reconnaissance légale aux signatures électroniques, en ne touchant toutefois pas aux autres notions du droit de la preuve telles que celles d'écrit, d'original ou d'acte sous seing privé. Elle s'est inscrite dans une certaine continuité en reprenant les concepts existants et en les ouvrant aux nouvelles technologies⁸.

⁴ Communication de la Commission au Conseil, au Parlement européen, au comité économique et social et au comité des régions : « Assurer la sécurité et la confiance dans la communication électronique – Vers un cadre européen pour les signatures numériques et le chiffrement », COM (97)503, adoptée le 7 octobre 1997.

⁵ Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L. 13 du 19 janvier 2000, pp. 12-20.

⁶ E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », in *La preuve*, Liège, Formation permanente CUP, vol. 54, 2002, p. 43.

⁷ *Ibid.*

⁸ M. ANTOINE et D. GOBERT, « La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur Internet », *J.T.*, n° 68, 2000, p. 78.

Les États membres ont procédé à la transposition de cette directive dans leur droit national, tout en veillant à concilier les exigences contenues en son sein avec le droit commun de la preuve⁹.

SECTION 2. – Les lois belges du 20 octobre 2000 et du 9 juillet 2001 transposant la directive 1999/93/CE

5.- **Transposition de la directive.** Les principes de la directive 1999/93/CE ont été transposés en droit belge par deux textes : la loi du 20 octobre 2000 et la loi du 9 juillet 2001. Le premier texte a une portée générale et introduit dans le Code civil une définition fonctionnelle de la signature électronique. Le second texte est quant à lui plus technique et définit les différents procédés de signature électronique en précisant partiellement les effets juridiques qu'il convient de leur accorder.

§ 1. L'article 1322, alinéa 2, du Code civil

6.- **Approche fonctionnelle.** La loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire¹⁰ a inséré à l'article 1322 du Code civil un second alinéa formulé comme suit :

« Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte ».

À l'avenir, cet article du Code civil a vocation à coexister avec le nouveau Règlement eIDAS¹¹. Dès lors, nous précisons ci-après les exigences qu'il pose en matière de signature électronique, son champ d'application ainsi que les effets juridiques qu'il confère à de telles signatures et donnons quelques exemples d'applications jurisprudentielles qui en ont été faites.

⁹ D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, p. 115.

¹⁰ Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000, p. 42698.

¹¹ Voy. *infra*, nos 40 et 41.

A. Les exigences d'imputabilité et d'intégrité du contenu de l'acte

7.- **Exigences posées par l'article 1322 du Code civil.** Deux exigences sont posées par le second alinéa de l'article 1322 du Code civil pour qu'une signature électronique puisse être assimilée à une signature manuscrite.

Premièrement, la signature doit être imputable à son auteur. Cela implique qu'elle permette d'identifier le signataire, que l'on puisse s'assurer de l'identité de l'interlocuteur. Par ailleurs, bien que la fonction d'adhésion au contenu de l'acte ne soit pas inscrite telle quelle dans le texte, elle « y figure implicitement sous la notion d'imputabilité éclairée par les travaux préparatoires, et se déduit, du reste, de la théorie générale de la signature »¹². Il est regrettable que le législateur ait introduit une définition fonctionnelle qui ne reprenne pas expressément toutes les fonctions de la signature¹³. Néanmoins, le juge est tenu d'apprécier si le signataire, lors de la signature de l'acte, avait la volonté de souscrire au contenu de celui-ci, tout en sachant qu'à l'instar de ce qui existe pour la signature manuscrite, le signataire qui reconnaît avoir signé électroniquement un document est présumé avoir donné son consentement au contenu de celui-ci¹⁴.

Deuxièmement, le second alinéa de l'article 1322 du Code civil requiert de la signature électronique qu'elle permette de maintenir l'intégrité du contenu de l'acte. Cela signifie qu'une fois l'acte signé, celui-ci ne doit plus pouvoir faire l'objet de modifications. Pourtant, le maintien de l'intégrité de l'acte n'est pas une fonction traditionnellement reconnue à la signature manuscrite. Traditionnellement, la doctrine s'accorde pour reconnaître deux fonctions à la signature manuscrite. D'une part, la signature sert à identifier son auteur et, d'autre part, elle sert à marquer son adhésion au contenu de l'acte¹⁵. La signature doit donc permettre l'identification certaine de son auteur et traduire sa volonté d'adhérer à l'acte.

¹² E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 69 et justification de l'amendement n° 12 du gouvernement à la Proposition de loi introduisant de nouveaux moyens de télécommunications dans la procédure judiciaire et extrajudiciaire du 13 juin 2000, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0038/006, p. 11 et le rapport fait au nom de la Commission de la justice par Bart Somers le 30 juin 2000, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0038/008, p. 30.

¹³ La fonction d'adhésion au contenu de l'acte traditionnellement reconnue à la signature ne ressort pas du second alinéa venu compléter l'article 1322 du Code civil alors qu'elle est précisément la raison pour laquelle la signature est apposée. Comme le note E. Montero, cette lacune est d'autant plus regrettable que « cette fonction apparaissait clairement dans la première version de la proposition de directive et également dans une version antérieure de l'alinéa 2 de l'article 1322 ». (E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 69)

¹⁴ M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », note sous Cass., 28 juin 1982, *R.C.J.B.*, 1985, pp. 69-70.

¹⁵ Cass., 30 avril 1942, *Pas.*, 1942, I, p. 103.

(D. MOUGENOT, « La preuve », *Rép. not.*, t. IV, I. II, Bruxelles, Larcier, 2002, pp. 188-189). L'insertion par le législateur de cette exigence supplémentaire a par conséquent été critiquée par la majorité de la doctrine¹⁶. Pour de plus amples précisions à ce sujet, nous renvoyons aux points nos 11 et 12.

En optant pour une approche fonctionnelle de la signature électronique, le législateur belge s'assure que celle-ci demeurera adaptée malgré l'évolution rapide des technologies. Toutefois, un tel choix a pour effet de confier aux magistrats la responsabilité d'apprécier, au cas par cas, si le procédé de signature utilisé rencontre les fonctions édictées à l'article 1322, alinéa 2, du Code civil.

8.- Champ d'application. Quant au champ d'application de l'article 1322 du Code civil, le doute plane sur l'étendue qu'il convient de lui reconnaître. Situé dans le Code civil sous la section relative à la preuve littérale, certains considèrent qu'il a pour vocation de s'appliquer à tous les actes sous seing privé, mais qu'il ne déroge pas aux régimes spécifiques prévoyant des obligations supplémentaires¹⁷. Sa portée serait limitée au droit de la preuve¹⁸. Cette disposition déterminerait donc uniquement les conditions dans lesquelles un acte sous seing privé signé électroniquement possède une certaine force probante¹⁹.

Néanmoins, la situation a changé avec l'entrée en vigueur de la loi du 11 mars 2003. Si, dans l'intervalle, cette loi a été abrogée pour être intégrée dans le Code de droit économique, on y retrouve toujours l'article XII.15 qui stipule que :

« § 1^{er}. Toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées.

§ 2. Pour l'application du § 1^{er}, il y a lieu de considérer : que l'exigence, expresse ou tacite, d'une signature est satisfaite dans les conditions prévues soit à l'article 1322, alinéa 2, du Code civil, soit à l'article 4, § 4 de la loi du 9 juillet 2001 ».

Compte tenu de la formulation de cet article, « le régime mis en place à l'article 1322 et à l'article 4, § 4 de la loi du 9 juillet 2001 est étendu au formalisme non probatoire »²⁰. En ce sens, P. Van Ommeslaghe note qu'« il n'est pas possible de donner des définitions différentes de la signature selon que l'on examine la force probante d'un acte ou tout autre condition dépendant de la signature »²¹. L'article 1322, alinéa 2 du Code civil pourrait donc, selon une certaine doctrine, trouver à s'appliquer tant dans un cadre probatoire que sur le terrain de la validité des actes juridiques²². En outre, selon E. Montero, « le principe consacré à l'article 1322, alinéa 2 du Code civil peut être étendu à toutes les branches du droit »²³.

L'article XII.16 du Code de droit économique limite toutefois le champ d'application de l'article XII.15 du Code de droit économique en ce qu'il prévoit que ce dernier article n'est pas applicable à différents types de contrats tels que :

- « 1° les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location ;
- 2° les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique ;
- 3° les contrats de suretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ;
- 4° les contrats relevant du droit de la famille ou du droit des successions ».

9.- Effets juridiques. Dans une perspective probatoire, il faut distinguer la force probante qu'il convient d'accorder à une signature électronique selon que celle-ci est contestée ou non. Si la validité de la signature électronique n'est pas remise en cause devant le juge, celui-ci lui reconnaîtra

¹⁶ En ce sens voy. not. E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 68 ; M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, coll. CRIDS, Bruxelles, Larcier, 2014, p. 592 ; *contra* : voy. not. P. VAN EECHE, « De elektronische handtekening in het recht », *R.D.C.*, 2009, p. 330.

¹⁷ E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 53 ; *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0038/008, p. 29 : « il n'est pas touché aux dispositions spécifiques relatives à la preuve ou aux prescriptions concernant la forme de certaines obligations issues de contrats, telles que prévues par le Code civil lui-même ou par une réglementation spécifique ».

¹⁸ En ce sens, H. JACQUEMIN, « Les formes applicables à certains contrats conclus par voie électronique », in M. DEMOULIN (coord.), *Les pratiques du commerce électroniques*, coll. CRIDS, n° 30, Bruxelles, Bruylant, 2007, p. 141 ; E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 39.

¹⁹ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », in *Pas de droit sans technologie*, CUP, vol. 158, Bruxelles, Larcier, 2015, p. 48.

²⁰ D. MOUGENOT, « La preuve », *Rép. not.*, t. IV, I. II, Bruxelles, Larcier, 2012, p. 216 ; voy. égal. H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 49.

²¹ P. VAN OMMESLAGHE, *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, coll. UB³, Bruxelles, Bruylant, 2012, p. 33.

²² *Ibid.*, p. 33 ; D. MOUGENOT, « La preuve », *op. cit.*, p. 216.

²³ E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 56 ; en sens contraire voy. P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique », in *Le commerce électronique : un nouveau mode de contracter ?*, Liège, Édition du Jeune Barreau, 2001, pp. 128-129.

des effets juridiques identiques à ceux d'une signature manuscrite. Le document fera pleine foi de son contenu. Par contre, si la signature est contestée par une partie au litige, le juge devra examiner si les conditions énumérées à l'article 1322, alinéa 2 du Code civil sont rencontrées. Si la recevabilité des signatures électroniques en justice s'en trouve assurée, il appartient au justiciable de convaincre le juge de la valeur probante de la signature apposée²⁴. Lorsque la signature satisfait aux conditions, le juge doit reconnaître à l'écrit électronique signé la force probante d'un acte sous seing privé²⁵. À l'inverse, si le juge considère que les conditions reprises à l'alinéa 2 de l'article 1322 du Code civil ne sont pas réunies, il pourra encore qualifier l'acte de présomption ou de commencement de preuve par écrit si celui-ci émane de la partie à laquelle on l'oppose et s'il rend vraisemblable le fait allégué²⁶. Toutefois, les effets juridiques qui seront attachés à ce type de preuve seront plus incertains étant donné qu'aucune force probante n'est reconnue aux présomptions et aux commencements de preuve par écrit. En outre, l'appréciation du juge est souveraine quant à la valeur probante qu'il convient de leur accorder. À cet égard, précisons que la personne qui se prévaut d'un commencement de preuve par écrit peut toujours tenter de démontrer que celui-ci est intègre, malgré que cette fonction d'intégrité ne soit pas assurée par la signature en elle-même. Dans cette perspective, les potentiels effets juridiques de ces modes de preuve « inférieurs » ne sont dès lors pas à négliger.

10.- Applications jurisprudentielles. Dans une affaire qui opposait une caisse d'assurances sociales pour indépendants à un de ses affiliés, la Cour du travail de Bruxelles a été amenée à examiner le mode de signature utilisé par la caisse d'assurances sociales, pour signer les courriers recommandés envoyés à ses affiliés, en vue d'interrompre la prescription de son action en recouvrement des cotisations sociales impayées²⁷. La caisse d'assurances sociales avait en effet développé une pratique

²⁴ Exposé des motifs du projet de loi relatif à l'activité des prestataires de services de certification en vue de l'utilisation de signatures électroniques, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0322/001, p. 14 ; E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 45.

²⁵ Amendement n° 12 du Sénateur Paul DE GRAUWE (daté du 18 avril 2001), *Doc. parl.*, Sén., sess. 2000-2001, n° 2-662/2 et E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, pp. 60-62.

²⁶ M.E. STORME, « De invoering van de elektronische handtekening in ons bewijsrecht. Een inkadering van een commentaar bij de nieuwe wetsbepalingen », *R.W.*, 2000, n° 59 et 60.

²⁷ C. trav. Bruxelles, 11 octobre 2013 et C. trav. Bruxelles, 14 février 2014, *R.D.T.I.*, 2014, pp. 115-121 ; pour un commentaire détaillé de ces décisions voy. J.-B. HUBIN, « Signature scannée : quand une technologie simple confronte le juriste à des questions complexes », *R.D.T.I.*, 2014, pp. 122-134 ; voy. égal. K. ROSIER, « La signature scannée : quelle valeur sur le plan juridique ? », *Bull. Social et juridique*, 2013, p. 516.

consistant à apposer par voie informatique, sur les courriers interruptifs de prescription, la signature de la personne compétente, après l'avoir scannée et l'avoir enregistrée dans une base de données. Dans le cadre du litige dévolu à la Cour du travail de Bruxelles, le travailleur indépendant poursuivi mettait en cause ce processus de signature, considérant que la signature scannée ne pouvait être assimilée à une signature au sens de l'article 1322 du Code civil et affirmant, en conséquence, que l'action en réclamation des cotisations sociales dues était prescrite.

Dans cet arrêt du 11 octobre 2013, la Cour du travail de Bruxelles a d'abord affirmé que la signature scannée constituait une signature électronique ordinaire au sens de la loi du 9 juillet 2001. Elle a ensuite exposé les fonctions que devait rencontrer la signature électronique pour permettre son assimilation à une signature manuscrite. En application de l'article 1322, alinéa 2 du Code civil, la Cour se devait d'apprécier si la signature scannée utilisée rencontrait les fonctions d'identification et d'adhésion dévolues à la signature, et de vérifier si la fonction d'intégrité avait été respectée. Au terme de son analyse, la Cour du travail a invité la caisse d'assurances sociales à établir que le processus de signature remplissait de telles fonctions. Dans cette perspective, la caisse d'assurances sociales était appelée à préciser qui pouvait accéder au fichier électronique contenant la signature numérisée et à démontrer qu'il n'était pas techniquement possible d'y accéder autrement que grâce à un mot de passe personnel. Ce premier arrêt faisait une correcte application des principes établis par l'article 1322 du Code civil.

Après une réouverture des débats, la Cour du travail de Bruxelles a rendu un second arrêt dans lequel, au lieu de répondre aux questions techniques qu'elle avait elle-même soulevées, de manière pertinente, elle a limité son analyse à l'examen d'une attestation produite par la caisse d'assurances sociales et émanant de la personne dont la signature scannée avait été employée. La Cour a déduit de cette attestation qu'il était certain que la signature figurant sur la lettre recommandée était bien celle de cette personne²⁸. Elle a estimé, dans la foulée, que l'apposition de cette signature scannée marquait effectivement l'adhésion de la personne au contenu de la lettre. Par ailleurs, alors qu'elle avait rappelé la fonction d'intégrité dans son arrêt du 11 octobre 2013, la Cour du travail de Bruxelles a, de manière critiquable, laissé sans réponse la deuxième exigence – certes controversée²⁹ – imposée par l'article 1322, alinéa 2 du Code civil. Nous estimons que la Cour aurait dû être plus exigeante sur ce point avec la caisse d'assurances sociales. Elle aurait dû l'inviter à démontrer que le procédé qu'elle avait utilisé assurait le maintien de

²⁸ *Contra* : voy. Trib. Police, Flandre occidentale (Section Bruges), 8 février 2016, inédit.

²⁹ Voy. *infra*, n° 11 et 12.

l'intégrité du contenu de la lettre recommandée. La Cour a jugé, pour le surplus, que compte tenu de la production de cette attestation, les explications techniques qu'elle avait elle-même souhaité obtenir étaient superflues. On regrettera qu'au contraire, la Cour du travail de Bruxelles n'ait pas poursuivi l'examen technique du processus informatique utilisé par la caisse d'assurances sociales³⁰. Il s'agissait, en effet, du seul moyen de vérifier que la signature électronique employée remplissait les fonctions d'imputabilité et d'intégrité nécessaires à son assimilation à une signature manuscrite.

Le Conseil de discipline des barreaux francophones du ressort de la cour d'appel de Bruxelles a également été confronté à une affaire, en matière disciplinaire, dans laquelle une partie invoquait l'irrecevabilité des poursuites à son encontre, au motif que la plainte disciplinaire n'avait pas été signée, alors qu'une telle formalité est exigée par l'article 458, § 1^{er}, du Code judiciaire³¹. L'affaire trouvait en effet son origine dans une plainte envoyée par e-mail, simplement revêtue du nom de son auteur. Le Conseil de discipline a d'abord rappelé que la signature devait, en principe, être manuscrite, sous réserve des exceptions prévues par la loi. Il a ensuite poursuivi son raisonnement, après avoir fait référence à l'article 1322 du Code civil, en précisant que « le juge, saisi d'une signature électronique, doit vérifier si elle peut être accueillie comme une signature au sens civil du terme et apprécier, *in concreto*, si elle répond aux conditions d'identification de la personne, de son imputabilité et de son adhésion au contenu de l'acte. En faisant application de ces principes au cas d'espèce, le Conseil de discipline a estimé que l'ensemble des données électroniques figurant dans l'e-mail contenant la plainte satisfaisait, au sens de l'article 1322, alinéa 2 du Code civil, aux exigences mentionnées ci-avant et en a déduit que « l'ensemble de ces données pouvait être assimilé, sans aucun doute possible, à une signature traditionnelle ».

Si l'on salue l'analyse des principes proposée par le Conseil de discipline afin de déterminer s'il a été saisi régulièrement, on regrette toutefois qu'il n'ait pas procédé à un examen des caractéristiques techniques du procédé de signature lui permettant de vérifier si celui-ci satisfaisait effectivement aux exigences requises pour être jugé équivalent à une signature manuscrite. En outre, dans son énonciation des conditions que doit remplir la signature électronique pour être assimilée à une signature manuscrite, le Conseil nous

³⁰ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 74 ; J.-B. HUBIN, « Signature scannée : quand une technologie simple confronte le juriste à des questions complexes », *op. cit.*, pp. 122-134.

³¹ Conseil de discipline des barreaux francophones du ressort de la cour d'appel de Bruxelles, 4 avril 2014, *J.L.M.B.*, 2014, pp. 937-941.

paraît mentionner certaines fonctions de manière redondante. En effet, de la fonction d'imputabilité découle l'identification de la personne ainsi que son adhésion au contenu de l'acte³². Le Conseil ne fait par ailleurs aucune référence à la fonction du maintien de l'intégrité du contenu de l'acte bien qu'il se réfère expressément à l'article 1322, alinéa 2 du Code civil.

B. L'exigence du maintien de l'intégrité du contenu de l'acte, une exigence discriminatoire ?

11.- Intégrité du contenu de l'acte. En insérant l'article 1322, alinéa 2 au sein de Code civil, le législateur belge a requis, pour qu'une signature électronique soit assimilée à une signature manuscrite, qu'elle permette de maintenir l'intégrité du contenu de l'acte auquel elle est liée. Cet alinéa se borne à énoncer les exigences auxquelles doit répondre une signature dans l'environnement numérique pour se substituer utilement à une signature manuscrite. En effet, si l'article 1322 du Code civil donne une définition fonctionnelle de la signature électronique, il ne propose cependant pas une définition fonctionnelle de la signature en général³³.

Contrairement aux fonctions rencontrées par la signature manuscrite dans l'environnement traditionnel – qui consistent à permettre l'identification du signataire de l'acte et à marquer son adhésion au contenu de l'acte – dans le monde numérique la signature électronique semble devoir assurer une fonction complémentaire. Pour voir conférer des effets juridiques à la signature électronique, sur le terrain de la preuve des actes sous seing privé, ceci implique qu'il faille que l'acte signé électroniquement n'ait pas été modifié entre le moment de sa conception et celui de sa réception par le destinataire, ainsi que durant la période pendant laquelle il est archivé.

12.- Existence d'une discrimination ? En ajoutant cette exigence d'intégrité à l'article 1322, alinéa 2 du Code civil, le législateur belge ne crée-t-il pas une discrimination entre la signature manuscrite et la signature électronique ? La signature électronique doit en effet, pour être assimilée à une signature manuscrite, remplir davantage de fonctions que la signature manuscrite³⁴.

Cette exigence d'intégrité introduite par le législateur a fait l'objet de critiques de la part de la doctrine belge. Celle-ci considère en effet que l'ajout de cette condition est de nature à priver d'efficacité juridique la

³² Voy. *supra*, n° 7.

³³ P. LECOCQ et P. VANBRABANT, « La preuve du contrat conclu par voie électronique – clap 2^{ème} », *Act. Dr.*, 2002/3, p. 299.

³⁴ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 70.

majorité des signatures électroniques ordinaires³⁵. Dans l'environnement papier, c'est le support de l'*instrumentum* qui assure d'une certaine manière l'intégrité du contenu et non la signature en elle-même³⁶. Comme le précise L. Guinotte, « c'est la combinaison de ces deux éléments qui assure le maintien de l'intégrité des informations que le document contient »³⁷. En effet, le support papier permet de maintenir l'intégrité du document car il rend les modifications de l'écrit plus difficiles³⁸. La signature traditionnelle ne permet pas, en elle-même, le maintien de l'intégrité de l'acte. On pense notamment à l'hypothèse dans laquelle la signature est uniquement apposée sur la dernière page d'un document en contenant plusieurs. S'il est vrai que le mécanisme de signature électronique qui repose sur la cryptographie asymétrique assure, grâce à la fonction de hachage utilisée³⁹, le maintien de l'intégrité, il n'en va pas nécessairement de même de certains autres types de signature électronique⁴⁰.

En outre, en requérant que l'intégrité du contenu de l'acte soit assurée par la signature électronique, le législateur exclut la possibilité de démontrer par tout autre moyen que le document n'a pas été altéré. Un document dont l'intégrité a été conservée par un autre dispositif pourrait, en vertu de cette interprétation de l'article 1322, alinéa 2 du Code civil, ne pas être considéré comme un acte sous seing privé par le juge.

Dès lors, cette exigence supplémentaire paraît insérer dans notre droit une discrimination entre la signature électronique et la signature manuscrite. Elle semble par ailleurs contraire à l'objectif poursuivi par le législateur, qui est d'assurer la sécurité des relations contractuelles⁴¹. À cet égard, s'il est primordial que l'intégrité du contenu qui a été approuvé lors de la signature soit maintenue dans un environnement où les falsifications sont aisées⁴², on s'interroge néanmoins sur l'opportunité d'attribuer une telle fonction à la signature électronique⁴³. En ce sens, M. Demoulin considère

³⁵ E. MONTERO, « La signature électronique au banc de la jurisprudence », *D.A.O.R.*, 2011, p. 238.

³⁶ M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, op. cit., p. 591.

³⁷ L. GUINOTTE, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, n° 6063, 2002, p. 555.

³⁸ D. MOUGENOT, « La preuve », op. cit., pp. 205 et 218.

³⁹ Voy. *supra*, p. 12.

⁴⁰ L. GUINOTTE, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », op. cit., p. 555.

⁴¹ M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, op. cit., p. 592.

⁴² D. MOUGENOT « La preuve », op. cit., p. 219.

⁴³ Sur ce point, voy. aussi la contribution de H. Jacquemin (n° 22), dans le présent ouvrage.

d'ailleurs que l'« on déroge au principe d'équivalence fonctionnelle, dans la mesure où il y a asymétrie entre les qualités fonctionnelles de la signature manuscrite et de la signature électronique »⁴⁴.

Pour pallier à ces critiques, une autre lecture de l'article 1322, alinéa 2 du Code civil peut être proposée. Tel qu'il est formulé, cet alinéa n'exige pas que les fonctions d'imputabilité et de maintien d'intégrité du contenu de l'acte soient remplies par la signature électronique en elle-même, mais plutôt par « un ensemble de données électroniques ». En effet, l'article 1322 est formulé comme suit : « Peut satisfaire à l'exigence d'une signature (...) un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte ».

Cet ensemble de données électroniques pourrait être envisagé plus largement que comme étant exclusivement constitué d'une signature électronique. À la lecture du texte rien ne semble empêcher que cette signature soit complétée par d'autres données électroniques permettant de prouver que le document est intègre et émane de son auteur, lequel adhère à son contenu⁴⁵.

À cet égard, il apparaît que la jurisprudence, dans son appréciation de la valeur à reconnaître aux signatures électroniques, tient déjà compte de l'ensemble des éléments techniques qui entourent le procédé de signature électronique en tant que tel afin de déterminer si les exigences posées par l'article 1322, alinéa 2 du Code civil sont rencontrées. Certaines juridictions ont d'ailleurs déjà accepté que le maintien de l'intégrité du document soit démontré au moyen des processus techniques qui gravitent autour de la signature électronique⁴⁶.

Cette approche permet d'accorder des effets juridiques à une signature électronique qui, bien qu'elle ne remplisse pas intrinsèquement les fonctions énoncées à l'article 1322, alinéa 2 du Code civil⁴⁷, rencontre les

⁴⁴ M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, op. cit., p. 592.

⁴⁵ En ce sens, *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, n° 0038/006, p. 6 : « Dans le contexte électronique, l'inaltérabilité n'est plus assurée par le seul support. Certes, certains supports, (...) sont capables de contenir de l'information de façon indélébile. Il n'empêche que dans un environnement électronique, ce n'est pas tellement le support qui garantit l'inaltérabilité, mais bien le processus informatique utilisé, comme par exemple la signature digitale » (nous soulignons).

⁴⁶ Voy. *infra*, n° 13 et plus particulièrement la décision du Conseil contentieux étrangers, 19 novembre 2009, n° 34364, *www.rvv-cc.ee.be*. Voy. égal. E. MONTERO, « La signature électronique au banc de la jurisprudence », op. cit., p. 232.

⁴⁷ *Contra* : voy. J. DUMORTIER, « Elektronische handtekening : juridische en praktische aspecten », in *Assurances et technologies de l'information et de la communication*, Mechelen, Kluwer, 2014, p. 100, qui considère que les fonctions énumérées à l'article 1322, alinéa 2 du Code civil doivent être remplies par la signature électronique en elle-même et non par les procédés techniques adjacents.

objectifs poursuivis par le législateur. Une telle approche semble avoir été préconisée en droit civil français. L'article 1316-4 du Code civil français requiert en effet que l'intégrité de l'acte soit garantie mais n'exige pas qu'elle le soit au moyen de la signature électronique.

13.- Exemples tirés de la jurisprudence belge. À titre d'exemple, des décisions de refus d'accès au territoire ou d'éloignement émises par l'Office des étrangers ont fait l'objet de recours de la part de leurs destinataires au motif que celles-ci étaient signées au moyen d'une signature scannée⁴⁸. Le procédé consistait à numériser la signature manuscrite du fonctionnaire compétent et à l'apposer, à l'aide d'un logiciel, sur la décision relative à la personne étrangère. Une fois revêtue de la signature scannée, la décision était imprimée et envoyée à l'intéressé. Or, en cas de non-respect des formalités substantielles, une telle décision est susceptible d'être annulée⁴⁹. La validité de ces signatures fut donc remise en cause par les plaignants dans le cadre de recours en annulation de décisions.

Dans une décision du 8 mai 2009, le Conseil d'État a tout d'abord rejeté ce procédé de signature au motif que l'Office des étrangers n'avait pas su faire la preuve des mesures techniques mises en place afin d'assurer la fiabilité de la signature. L'Office des étrangers se révéla notamment impuissant à démontrer que cette forme de signature garantissait l'identité réelle et les fonctions de l'auteur de la décision⁵⁰. Ultérieurement, dans un arrêt du 19 novembre 2009⁵¹, dans le cadre duquel il était saisi d'une question similaire, le Conseil du contentieux des étrangers a rappelé qu'une signature scannée pouvait être qualifiée de signature électronique ordinaire au sens de l'article 2 de la loi du 9 juillet 2001. Après que l'Office des étrangers ait démontré que son usage des signatures scannées rencontrait les conditions fixées par l'article 1322, alinéa du Code civil, le Conseil du contentieux des étrangers a considéré que la signature scannée utilisée dans le cas d'espèce assurait à suffisance l'identification de son auteur, qu'elle matérialisait son adhésion au contenu du document

⁴⁸ Pour une analyse approfondie des décisions rendues en matière de signatures scannées, voy. J.-B. HUBIN, « Signature scannée : quand une technologie simple confronte le juriste à des questions complexes », *op. cit.*, pp. 122-134 ; Pour une analyse détaillée des décisions du Conseil du contentieux des étrangers du Conseil d'État à ce sujet, voy. E. MONTERO, « La signature électronique au banc de la jurisprudence », *op. cit.*, pp. 231-239 et J. VANDENDRIESCHE, « An overview of some recent case law in Belgium in relation to electronic signatures », *Digital Evidence and Electronic Signature Law Review*, 2010, pp. 90-100.

⁴⁹ J. VANDENDRIESCHE, « An overview of some recent case law in Belgium in relation to electronic signatures », *op. cit.*, p. 90. Signature 937-941.

⁵⁰ C.E., 8 mai 2009, n° 193.106, www.raadvst-consetat.be.

⁵¹ Conseil contentieux étrangers, 19 novembre 2009, n° 34364, www.rvv-cce.be.

signé et qu'elle présentait assez de garanties en termes de maintien de l'intégrité du document. Les informations techniques communiquées par l'Office des étrangers, démontrant que l'accès à la copie scannée de la signature du fonctionnaire compétent nécessitait l'emploi de login et de mots de passes personnels, ont été expressément mises en évidence par le Conseil du contentieux des étrangers. La rigueur de l'analyse technique réalisée par le Conseil du contentieux des étrangers mérite d'être soulignée. Cette motivation est d'ailleurs régulièrement rappelée par le Conseil dans le cadre d'autres affaires dans lesquelles la question de la valeur du processus de signature scannée utilisé par l'Office des étrangers est soulevée⁵².

Il ressort de cette jurisprudence, qu'en pratique, les magistrats, dans l'exercice de leur pouvoir d'appréciation de la valeur à reconnaître aux signatures électroniques, accordent de l'importance à l'ensemble des éléments qui leurs sont soumis. Comme le souligne E. Montero, « en matière de preuve électronique, cette appréciation (...) s'étend à l'ensemble du cycle de vie du document contesté. Autrement dit, c'est tout le processus de création-conservation-gestion du document numérique qui est pris en compte dans l'appréciation des preuves »⁵³.

§ 2. La loi du 9 juillet 2001

14.- Présentation. La loi du 9 juillet 2001, qui transpose en droit belge la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, fixe certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification⁵⁴. Cette loi propose une définition de différentes formes de signatures électroniques et énonce, en partie, les effets juridiques qu'il convient de leur conférer. Elle avait vocation à être intégrée dans le titre 2 du livre XII du Code de droit économique⁵⁵ qui doit traiter plus spécifiquement de certaines règles relatives au cadre juridique pour les signatures électroniques, l'archivage électronique, le recommandé électronique, l'horodatage électronique et les services de certification. À l'avenir, elle devrait toutefois être abrogée au profit, d'une part, du Règlement eIDAS et, d'autre part, de l'avant-projet

⁵² E. MONTERO, « La signature électronique au banc de la jurisprudence », *op. cit.*, p. 232.

⁵³ *Ibid.*, p. 236.

⁵⁴ Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001.

⁵⁵ Proposition de loi modifiant la législation en ce qui concerne l'instauration du droit de l'économie électronique, *Doc. parl.*, Ch. repr., sess. ord., 2012-2013, n° 2745/003, p. 3.

de loi mettant en œuvre et complétant le Règlement n° 910/2014⁵⁶ dont nous reparlerons par la suite.

15.- Champ d'application. Précisons d'emblée que le champ d'application de la loi du 9 juillet 2001 est plus étendu que celui de l'article 1322, alinéa 2, du Code civil en ce qu'il détermine le cadre juridique applicable en toutes matières pour les signatures électroniques⁵⁷. Le domaine d'application de la loi s'étend par exemple tant aux cas dans lesquels la signature est requise pour protéger une partie faible qu'à ceux dans lesquels elle est nécessaire à la sécurité des relations contractuelles⁵⁸.

Étant donné que, dans le cadre de la mise en œuvre du Règlement eIDAS, cette loi sera prochainement abrogée, nos propos à son sujet dans le chapitre suivant resteront succincts et auront pour objectif de comparer le cadre normatif belge qui régit actuellement la matière de la signature électronique avec les nouvelles dispositions du Règlement eIDAS. Pour le surplus nous renvoyons aux nombreuses contributions déjà consacrées à l'examen de la loi du 9 juillet 2001⁵⁹.

⁵⁶ Avant-projet de loi mettant en œuvre et complétant le Règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, version du 11 décembre 2015, disponible sur <http://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2015&num=702>, consulté le 12 février 2016.

⁵⁷ D. MOUGENOT, « La preuve », *op. cit.*, pp. 213-214 ; P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique – *clap 2^{ème}* », *op. cit.*, p. 296 ; M. DEMOULIN et E. MONTERO, « Le formalisme contractuel à l'heure du commerce électronique », in *Commerce électronique : de la théorie à la pratique*, Bruxelles, Bruylant, 2003, p. 186.

⁵⁸ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 47.

⁵⁹ D. GOBERT, « Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001 », in *La preuve*, Liège, Formation permanente CUP, vol. 54, 2002, pp. 83-172 ; J. VANDENDRIESSCHE, « De elektronische handtekening », *op. cit.*, pp. 1-57 ; D. MOUGENOT, « La preuve », *op. cit.*, p. 212. ; E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, pp. 39-82.

CHAPITRE II. Analyse des nouvelles dispositions applicables aux signatures électroniques suite à l'adoption du Règlement eIDAS

16.- Ratio legis du Règlement eIDAS. Il y a quinze ans, le législateur européen s'était focalisé sur la manière de réaliser et de reconnaître les signatures électroniques. Aujourd'hui, dans le Règlement 910/2014, les autorités européennes ne traitent plus uniquement de la signature électronique. Elles ont défini un cadre juridique s'appliquant à l'offre des services qui interviennent au moment de la conclusion, de la transmission et de la conservation d'un acte juridique dans un processus totalement électronique⁶⁰. Le Règlement s'intéresse donc au cycle de vie complet du document électronique ainsi qu'aux différents intervenants y prenant part. Pour développer la confiance dans l'économie numérique, il est en effet primordial de garantir la fiabilité de ces services mais également de veiller à garantir la validité et la preuve de l'acte juridique conclu électroniquement à l'aide de ces services⁶¹.

À partir du 1^{er} juillet 2016, chaque citoyen européen utilisant des services électroniques de signatures mais aussi d'horodatage, de recommandés et d'authentification de site internet bénéficiera des effets juridiques conférés par le Règlement à chacun de ces services de confiance qualifiés et non qualifiés. Les juridictions de chaque pays européen seront en outre tenues de leur reconnaître ces effets juridiques⁶².

SECTION 1. – Le nouveau cadre juridique prévu par le Règlement eIDAS

17.- Présentation. Dans les sections 4 et 5 de son chapitre 3 relatif aux services de confiance, le Règlement établit les nouvelles règles applicables au sein de l'Union européenne en matière de signatures et de cachets électroniques. Bien que les dispositions relatives au cachet électronique soient similaires à celles applicables à la signature électronique, leur analyse fait

⁶⁰ D. GOBERT, « Le Règlement européen du 23 juillet 2014 sur les services d'identification électronique et les services de confiance (eIDAS) : évolution ou révolution ? », *R.D.T.I.*, 2014, n° 56, p. 36.

⁶¹ *Ibid.*

⁶² *Ibid.*, p. 37.

l'objet, en raison de leur caractère novateur, d'un titre distinct au sein du présent ouvrage.

§ 1. Clarification des principes de non-discrimination et d'assimilation

Tout en rappelant ponctuellement le régime légal actuel, l'accent est mis dans les développements qui suivent sur les nuances et les nouveautés apportées par le Règlement eIDAS.

A. Principe d'assimilation

18.- En droit national. En droit belge, l'article 4, § 4, de la loi du 9 juillet 2001 stipule que :

« Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale ».

En établissant les conditions dans lesquelles une signature électronique doit être assimilée à une signature manuscrite, cet article consacre le principe d'assimilation dans notre droit national. Lorsqu'un procédé de signature électronique rencontre l'ensemble de ces exigences – hypothèse dans laquelle il est alors appelé communément par la doctrine « signature électronique qualifiée » – il est assimilé automatiquement à une signature manuscrite⁶³.

On relève d'ores et déjà que la possibilité de signer électroniquement a été expressément accordée aux personnes morales. Pour de plus amples développements concernant cette faculté, nous renvoyons au titre qui est consacré au cachet électronique dans cet ouvrage, la signature électronique étant à l'avenir réservée aux seules personnes physiques.

19.- En droit européen. Le Règlement reprend le principe d'assimilation en vertu duquel le juge doit assimiler le procédé de signature électronique qualifiée à une signature manuscrite⁶⁴. En effet, en son alinéa 2, l'article 25 du Règlement précise que la signature électronique qualifiée doit se voir reconnaître des effets juridiques équivalents à ceux d'une signature manuscrite. Pour le reste, il revient au législateur national de définir l'effet juridique produit par les signatures manuscrites.

⁶³ D. MOUGENOT, « La preuve », *op. cit.*, p. 212.

⁶⁴ À ce sujet, voy. égal. le point 35 de la contribution de H. Jacquemin.

20.- Effets juridiques. Le Règlement ne se prononce pas sur les effets juridiques à donner aux signatures électroniques, à l'exception de la valeur particulière qu'il convient d'accorder aux signatures électroniques qualifiées. Dans une perspective probatoire, si les conditions de la signature électronique qualifiée sont rencontrées, celle-ci bénéficie du principe d'assimilation et aura la même valeur qu'une signature manuscrite. L'acte sur lequel est apposée la signature électronique qualifiée est donc à considérer comme un acte sous seing privé faisant pleine foi de son contenu, sous réserve d'une procédure en vérification d'écriture. Par contre, si la signature électronique utilisée ne peut être considérée comme « qualifiée », le juge devra se livrer à un examen de la signature électronique sous l'angle de l'article 1322, alinéa 2, du Code civil et apprécier si le procédé utilisé remplit les fonctions reconnues à la signature. Si ces fonctions ne sont pas remplies, la signature électronique ne pourra être assimilée à une signature manuscrite.

Concernant l'articulation des deux textes, il ressort des travaux préparatoires de la loi du 9 juillet 2001, que « le projet relatif aux autorités de certification accorde force probante aux signatures électroniques avancées créées par un dispositif sécurisé de création de signature et combinées à un certificat qualifié. Ces signatures bénéficient des mêmes effets juridiques que ceux qui sont reconnus aux signatures manuscrites (...) Par contre, le projet relatif au droit de la preuve se limite à créer le principe de la recevabilité de tout type de signature, même électronique, le juge étant alors libre d'apprécier la valeur probante à accorder à celle-ci (il pourrait très bien accorder une valeur probante équivalente à celle de la signature manuscrite s'il estime que les différentes fonctions de la signature sont réalisées avec une certitude raisonnable) »⁶⁵.

B. Principe de non-discrimination⁶⁶

21.- Simplification. Le Règlement consacre également le principe de non-discrimination, déjà prévu à l'article 4, § 5, de la loi du 9 juillet 2001⁶⁷. Cette disposition transposait la clause de non-discrimination prévue par la directive 1999/93 dans notre droit.

⁶⁵ Doc. parl., Ch. repr., sess. ord., 1999-2000, n° 50 322/001, p. 13.

⁶⁶ Voy. égal. à ce sujet les points 10 et suivants de la contribution de H. Jacquemin.

⁶⁷ L'article 4, § 5, de la loi du 9 juillet 2001 est formulé comme suit « une signature électronique ne peut être refusée en justice au seul motif qu'elle se présente sous une forme électronique, qu'elle ne repose pas sur un certificat qualifié, ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature ».

En vertu de ce principe, une signature électronique ne peut être refusée en justice au seul motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de la signature électronique qualifiée⁶⁸. Le recours aux termes « signature électronique qualifiée » a permis de raccourcir et de rendre plus lisible la formulation du principe de non-discrimination. Par ailleurs, et contrairement au principe d'assimilation, la clause de non-discrimination bénéficie à tout type de signature électronique.

22.- Effet juridique. Il est important de comprendre que ce principe ne signifie pas qu'une signature électronique est, d'emblée, considérée comme équivalente à une signature manuscrite. Pour que tel soit le cas, « il faut démontrer que les fonctions de la formalité, telles qu'énoncées par le législateur ont été atteintes (le cas échéant, en se basant sur une clause d'assimilation) »⁶⁹. Ainsi, si, en vertu du principe de non-discrimination, la recevabilité d'une signature électronique en justice est certaine, son assimilation à une signature manuscrite (avec les effets juridiques qui en découlent) n'est toutefois qu'une possibilité réservée au juge qui appréciera la mesure dans laquelle les fonctions de la signature sont remplies (sauf s'il s'agit d'une signature électronique qualifiée).

§ 2. Graduation entre les signatures électroniques

23.- Différentes catégories de signatures. Le Règlement opère une claire distinction entre trois catégories de signatures électroniques, à savoir, la signature électronique ordinaire, avancée et qualifiée. On ne parlera plus à l'avenir de « signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature », mais simplement de « signature électronique qualifiée ». Si ce vocable était déjà utilisé fréquemment par la majorité des auteurs de doctrine, il est maintenant consacré par le législateur européen lui-même.

A. La signature électronique ordinaire

24.- Sous l'empire de la directive. Au sens de la directive 1999/93/CE et de la loi du 9 juillet 2001, la signature électronique simple ou ordinaire est entendue comme étant « une donnée sous forme électronique jointe ou

⁶⁸ Considérant n° 49 du Règlement eIDAS.

⁶⁹ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 61.

liée logiquement à d'autres données électroniques et servant de méthode d'authentification »⁷⁰. Une telle signature est recevable en justice en vertu du principe de non-discrimination⁷¹. Celui qui s'en prévaut devra, si elle est contestée, prouver que les conditions prévues à l'article 1322, alinéa 2 du Code civil sont remplies pour se voir reconnaître les mêmes effets juridiques qu'une signature manuscrite. Les conditions énumérées dans ce dernier article sont plus strictes que celles prévues à l'article 2, alinéa 2, 1° de la loi du 9 juillet 2001⁷². Comme le souligne E. Montero, l'article 1322, alinéa 2, du Code civil « conçoit l'identification d'une personne dans ses rapports avec un document dont elle s'approprie le contenu » tandis que la définition de la signature électronique « simple » reprise dans la loi du 9 juillet 2001 désigne toute méthode d'authentification⁷³, terme dont la portée est discutée⁷⁴ mais qui, à notre sens, doit à tout le moins être compris comme une méthode permettant de s'assurer de l'identité de la personne qui appose la signature. Dans un souci de clarification, la définition

⁷⁰ Art. 2.1, al. 2, 1° de la directive 1999/93/CE.

⁷¹ Art. 4, § 5, de la loi du 9 juillet 2001.

⁷² E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 52.

⁷³ *Ibid.*, p. 51.

⁷⁴ Pour E. Montero, l'authentification ne conduit pas nécessairement à l'identification d'une personne. Cette notion n'implique par ailleurs pas nécessairement que le contenu du document ait été approuvé (E. MONTERO, « Définition des effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 51). Cependant, D. Mougenot avance que, si l'on se réfère à la définition de l'authentification du dictionnaire juridique Cornu, l'authenticité s'entend comme « la qualité d'un objet ou d'un document dont l'auteur ou l'origine sont attestés, notamment sur la foi d'un certificat ». En ce sens, la signature électronique ordinaire sert donc à « vérifier que l'identité de l'auteur du document est bien garantie » (D. MOUGENOT, « La preuve », *op. cit.*, n° 122-2, p. 213). Pour P. Lecocq et B. Vanbrabant, le recours au terme d'authentification « paraît déborder de la fonction d'identification, dans la mesure où il ne se rapporte pas nécessairement à une personne ». À leur sens, l'authentification consiste dans la détermination de l'origine des données (qui peut être une personne mais aussi une machine) (P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique – clap 2^{ème} », *op. cit.*, p. 289). Aux yeux de H. Jacquemin, la fonction d'authentification est secondaire à la fonction d'adhésion au contenu de l'acte. Il s'agit d'une condition d'efficacité de la fonction d'adhésion. « En effet, la signature ne peut manifester la volonté de son auteur de s'approprier le contenu de l'acte si ce n'est pas lui, mais un tiers, qui a accompli la formalité » (H. JACQUEMIN, *Le formalisme contractuel : mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, p. 112). Si, comme le laisse entendre les travaux préparatoires (*Doc. parl.*, Ch. repr., sess. 1999-2000, n° 50-322, pp. 18-19), la signature électronique simple n'avait pas pour fonction d'identifier le signataire de l'acte, mais seulement d'authentifier le contenu de celui-ci, la notion de signature recevrait alors une portée totalement différente selon qu'elle s'applique dans l'environnement papier ou dans l'environnement numérique (H. JACQUEMIN, *Le formalisme contractuel : mécanisme de protection de la partie faible*, *op. cit.*, p. 355).

de la signature électronique ordinaire dans le Règlement eIDAS ne fait plus référence au terme « authentification »⁷⁵.

25.- Définition au sens du Règlement eIDAS. Le Règlement conserve une définition très large de la signature électronique. Est à considérer comme telle :

- des données sous forme électronique ;
- qui sont jointes ou associées logiquement à d'autres données sous forme électronique ;
- et que le signataire utilise pour signer⁷⁶.

Il ressort de la définition qu'un lien matériel fort doit exister entre l'acte et la signature. Il faut que les données de signature électroniques ne puissent être disjointes ou dissociées de l'acte auquel elles se rapportent. Cela s'explique par le fait que dans l'environnement traditionnel, c'est le papier qui assure le lien entre la signature et l'acte auquel celle-ci se rattache, mais dans l'environnement électronique, la signature électronique « peut avoir une existence autonome »⁷⁷. Il existe donc un risque que la signature soit dissociée du support auquel elle est initialement rattachée et que l'acte perde les effets juridiques qui sont susceptibles de lui être attachés⁷⁸. Le législateur européen a donc mis l'accent sur l'importance de l'existence d'un lien indissoluble entre la signature et l'acte électronique.

Par ailleurs, la signature électronique est désormais réservée aux seules personnes physiques⁷⁹. Les personnes morales devront recourir au cachet électronique⁸⁰.

26.- *Animus signandi*. Le signataire doit en outre avoir la volonté, en apposant les données électroniques, de signer. Comme le souligne H. Jacquemin, il est heureux que la fonction de « signer » ait été expressément ajoutée⁸¹. Le Règlement ne mentionne toutefois pas ce qu'il convient

⁷⁵ On retrouve toutefois à l'article 3.5 du Règlement une définition de la notion d'« authentification ». Celle-ci doit être entendue comme étant « un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique ».

⁷⁶ Art. 3.10 du Règlement eIDAS.

⁷⁷ D. MOUGENOT, « La preuve », *op. cit.*, p. 217.

⁷⁸ *Ibid.*

⁷⁹ Art. 3.9 du Règlement eIDAS.

⁸⁰ À ce sujet, voy. la contribution de J.-B. Hubin dans le présent ouvrage.

⁸¹ H. JACQUEMIN « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 72.

d'entendre par le terme « signer »⁸². Faut-il en déduire que signer signifie s'engager et que cette précision a été rajoutée afin de distinguer clairement la signature du cachet électronique auquel le Règlement n'accorde pas de pouvoir engageant ?⁸³ Ce silence peut en tout cas s'interpréter comme une volonté du législateur européen de laisser aux États membres la faculté de déterminer ce qu'implique le fait de signer. À cet égard, en Belgique, l'utilisation du mot « signer » renvoi aux fonctions traditionnellement reconnues par la doctrine et la jurisprudence à la signature. En effet, étant donné que la loi ne donne aucune définition de la signature, la Cour de cassation l'a définie comme étant « la marque manuscrite par laquelle le 'signataire' révèle habituellement sa personnalité aux tiers »⁸⁴. Traditionnellement, la doctrine s'accorde pour reconnaître deux fonctions à la signature manuscrite⁸⁵. D'une part, la signature sert à identifier son auteur et, d'autre part, elle sert à marquer son adhésion au contenu de l'acte⁸⁶. Dit autrement, en signant l'acte, le signataire s'approprie son contenu⁸⁷.

Dès lors, pour que des données sous forme électronique constituent une signature au sens du Règlement, il semble qu'il soit nécessaire que le signataire ait au moins la volonté de s'identifier et d'adhérer au contenu de l'acte. L'article 1322, alinéa 2 du Code civil va plus loin en ce qu'il exige en outre, pour qu'une signature électronique soit assimilée à une signature manuscrite, que l'ensemble de données électroniques maintienne le document intègre.

⁸² Dans une version de travail d'avril 2012, on retrouve une définition plus précise de la signature électronique qui est rédigée comme suit « *electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve for the signatory as : a) an expression of consent, or b) a method of authentication, or both a) and b)* » (T. PIETTE-CHODOL, « Règlement européen n° 910/2014 : le renouveau de la signature électronique et la consécration du cachet électronique », *RLDI*, février 2015, n° 112, p. 44.).

⁸³ Le choix est toutefois laissé à chaque État membre de déterminer si le cachet électronique a pour effet de manifester l'adhésion de la personne morale au contenu de l'acte. À ce sujet, voy. la contribution de J.-B. Hubin dans le présent ouvrage.

⁸⁴ Cass., 7 janvier 1995, *Pas.*, 1995, I, p. 456 ; Cass., 2 octobre 1964, *Pas.*, 1965, I, p. 106. Dans un arrêt ultérieur, la Cour de cassation a précisé que : « la signature d'un acte sous seing privé doit, en règle, être tracée directement sur le document lui-même » (Cass., 28 juin 1982, *Pas.*, 1982, I, p. 1286). Pour une analyse détaillée de la signature des actes sous seing privé, voy. M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », note sous Cass., 28 juin 1982, *R.C.J.B.*, 1985, pp. 57 et s.

⁸⁵ M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, *op. cit.*, pp. 587-593 ; D. MOUGENOT, « La preuve », *op. cit.*, pp. 188-189.

⁸⁶ Cass., 30 avril 1942, *Pas.*, 1942, I, p. 103.

⁸⁷ F. MOURLON-BEERNAERT, *La preuve en matière civile et commerciale*, Anvers, Kluwer, 2011, p. 107.

27.- **Effet juridique.** À l'instar de ce qui était prévu par la directive 1999/93/CE, le Règlement ne reconnaît aucune valeur juridique particulière à la signature électronique ordinaire. Il prévoit uniquement qu'en vertu du principe de non-discrimination qui sous-tend le Règlement, « l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée »⁸⁸. Ce principe de non-discrimination doit s'entendre largement et ne pas être cantonné au seul droit de la preuve⁸⁹.

En matière probatoire, il faut présumer que la force probante d'une telle signature est inexistante (ou faible) puisque le juge est libre d'en apprécier la valeur probante⁹⁰. Seule sa recevabilité ne peut être contestée. En cas de contestation d'une telle signature devant les tribunaux, il appartient à la partie qui s'en prévaut de démontrer que la signature a été utilisée pour signer, et donc que le procédé utilisé remplit les fonctions énumérées à l'article 1322, alinéa 2, du Code civil lorsque l'on tombe sous le champ d'application de cette disposition afin de convaincre le juge de lui donner des effets juridiques sur le plan probatoire⁹¹. Dans les hypothèses où cet article ne trouve pas à s'appliquer⁹², tout laisse à penser qu'il faudra se tourner vers les fonctions traditionnellement reconnues par la doctrine à la signature (identification et adhésion au contenu) et prouver que celles-ci sont rencontrées pour que des effets juridiques soient octroyés à la signature électronique ordinaire.

B. La signature électronique avancée

28.- **Définition au sens du Règlement eIDAS.** Le Règlement définit la signature électronique avancée comme étant une signature électronique qui doit :

- être liée au signataire de manière univoque ;
- permettre d'identifier le signataire ;

⁸⁸ Art. 25.1 du Règlement eIDAS.

⁸⁹ Si la formulation en français de ce principe peut créer le doute, les versions anglaise et néerlandaise confirment cette interprétation : « *An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures* » et « *Het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet* ».

⁹⁰ D. MOUGENOT, « La preuve », *op. cit.*, p. 223.

⁹¹ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, pp. 83-84.

⁹² Voy. not. les hypothèses énumérées à l'article XII.16 du code de droit économique.

- avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;
- être liée aux données associées à cette signature de sorte que toute modification ultérieure des données soit détectable.

29.- **Usage exclusif.** On soulignera que, sous l'empire de la directive, la signature électronique avancée devait être créée par des moyens que le signataire puisse garder sous son contrôle exclusif⁹³. Les signatures électroniques avancées devaient donc être créées dans un environnement entièrement géré par l'utilisateur et celui-ci devait prendre les mesures de sécurité lui permettant de garder la signature exclusivement sous son contrôle. Eu égard au fait qu'il est impossible pour tout type de signature électronique d'être gardée sous le contrôle exclusif d'une personne⁹⁴, on salue la modification qui est intervenue à cet égard dans le Règlement eIDAS. Désormais, le signataire peut avoir recours à un prestataire de service de signature électronique pour la création de ses données de signature. En effet, l'article 3.11 du Règlement est libellé en ce sens que la signature peut avoir été créée par autrui, du moment que le signataire conserve, avec un niveau de confiance élevé, l'usage de celle-ci sous son contrôle exclusif. La création de signatures électroniques à distance par un prestataire de services de confiance pour le compte du signataire doit être entourée de procédures de sécurité spécifiques⁹⁵. Par exemple, les canaux de communication électronique utilisés pour transmettre les signatures doivent être sécurisés afin de garantir que l'environnement de création des signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire. S'agissant de ce dernier point, cette obligation est en fait le corollaire de la première exigence qui requiert que la signature électronique avancée soit liée de manière univoque au signataire. Il est en effet primordial de pouvoir imputer avec certitude la signature à une personne spécifique, cette personne devant par ailleurs pouvoir être identifiée.

En outre, le Règlement requiert que toute modification apportée ultérieurement à un acte signé au moyen d'une signature électronique avancée soit détectable. On retrouve ici l'exigence du maintien de l'intégrité du contenu de l'acte qui était déjà requise en droit belge par l'article 1322

⁹³ Art. 2, 2) de la directive 1999/93/CE.

⁹⁴ S. MASON, *Electronic Signatures in Law*, 2^e éd., Tottel Publishing, 2007, p. 150 ; J. VANDENDRIESSCHE, « Hybrid signatures under Belgian Law », *Digital Evidence and Electronic Signature Law Review*, n° 9, 2012, p. 80, note 4.

⁹⁵ Considérant n° 52 du Règlement eIDAS.

du Code civil. Il s'agit d'une différence majeure qui existe entre la signature électronique ordinaire et la signature électronique avancée.

30.- Effet juridique. La signature électronique avancée ne se voit pas reconnaître plus d'effets juridiques que la signature électronique ordinaire. À la lecture du Règlement, il n'y a en effet pas de différence entre les deux quant aux effets juridiques à leur conférer. Toutefois, le juge, amené à apprécier la valeur d'une signature électronique, sera certainement plus enclin à accorder de la valeur probante à une signature électronique avancée, celle-ci reposant sur un procédé techniquement plus fiable qu'une signature électronique ordinaire.

C. La signature électronique qualifiée et son processus de validation

31.- Définition au sens du Règlement eIDAS. Sous l'empire du Règlement, le concept de signature électronique qualifiée est en grande partie conservé tel qu'il existait. Au sens du Règlement, la signature électronique qualifiée est :

- une signature électronique avancée ;
- qui est créée à l'aide d'un dispositif de création de signature électronique qualifié ;
- et qui repose sur un certificat qualifié de signature électronique⁹⁶.

Nous avons exposé au point précédent les exigences qui doivent être rencontrées pour qu'une signature électronique soit appelée « signature électronique avancée ». Deux éléments additionnels sont requis pour qu'une telle signature soit considérée comme étant une « signature électronique qualifiée ».

Premièrement, la signature doit avoir été créée à l'aide d'un dispositif de création de signature électronique qualifié. Le texte précise qu'il faut entendre par là, « un dispositif logiciel ou matériel configuré servant à créer une signature électronique »⁹⁷. Ce dispositif sera considéré comme étant « qualifié »⁹⁸ si :

(i) Il garantit au moins, par des moyens techniques et des procédés appropriés, que :

a) La confidentialité des données de création de la signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;

⁹⁶ Art. 3.12 du Règlement eIDAS.

⁹⁷ Art. 3.22 du Règlement eIDAS.

⁹⁸ Annexe II du Règlement eIDAS.

b) Les données de création de signature électronique utilisées pour créer la signature ne peuvent être pratiquement établies qu'une seule fois ;

c) L'on peut avoir l'assurance que de telles données ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;

d) Les données de création de la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

(ii) Il ne modifie pas les données à signer et n'empêche pas la présentation de ces données au signataire avant la signature.

(iii) Seul un prestataire de services de confiance qualifié peut s'être vu confier la génération et la gestion des données de création de signature électronique pour le compte du signataire.

(iv) Sans préjudice du paragraphe (i), d., un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte du signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes :

a) Le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;

b) Le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

Deuxièmement, la signature électronique doit reposer sur un certificat qualifié. Le Règlement précise à ce sujet qu'un certificat de signature électronique est « une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne »⁹⁹. Pour être reconnu comme « qualifié », ce certificat doit être délivré par un prestataire de services de confiance qualifié et répondre aux exigences énumérées à l'annexe I du Règlement.

Si, sur bien des points, le législateur européen laisse une marge de manœuvre aux États membres, il prévoit par contre une harmonisation complète quant aux exigences auxquelles doivent répondre les certificats qualifiés. En son considérant 54, il est en effet précisé que l'interopérabilité et la reconnaissance transfrontalière des certificats qualifiés sont une condition préalable à la reconnaissance transfrontalière des signatures électroniques qualifiées. Dès lors, les certificats qualifiés sur lesquels

⁹⁹ Art. 3.14 du Règlement eIDAS.

reposit de telles signatures ne peuvent faire l'objet d'aucune exigence allant au-delà de celles qui sont mentionnées dans le Règlement¹⁰⁰.

32.- Rôle des tiers de confiance. Dans le cadre de la présente contribution, le cadre légal général applicable à l'activité des prestataires de services de confiance n'est pas détaillé¹⁰¹. Précisons néanmoins que ces prestataires ont un rôle important à jouer car, comme le note D. Mougenot, « la confiance des utilisateurs ne pourra s'instaurer que si les transactions électroniques sont garanties par un tiers neutre »¹⁰². En matière de signature électronique, c'est eux qui vont fournir les procédés sur lesquels vont reposer les signatures. En effet, en tant que tiers de confiance, le prestataire va vérifier l'identité des titulaires de clé publique et générer des certificats qui établissent le lien entre la personne et sa clé publique.

33.- Cryptographie asymétrique. La description des exigences technologiques requises pour qu'une signature électronique soit « qualifiée » est très détaillée et, bien qu'elle tente de ne pas se limiter à un procédé spécifique, il ressort de sa lecture qu'actuellement seule la signature qui s'appuie sur la cryptographie asymétrique rencontre les impératifs requis. D. Mougenot considèrerait déjà, sous l'empire de la directive, que « cela n'était pas gênant parce que, autant la neutralité technologique doit être observée strictement dans l'application du principe de non-discrimination, autant le principe d'assimilation opère explicitement un choix technologique bien précis, offrant le plus haut degré de sécurité. Le fait que la définition de la signature électronique qualifiée (...) ne recouvre en définitive qu'un seul procédé de signature ne constitue donc pas une entorse à la Directive »¹⁰³. La signature électronique réalisée sur la base du certificat de signature contenu dans la puce de la carte d'identité électronique belge constitue un exemple d'une telle forme de signature.

34.- Avantages de la signature qualifiée. Faisant preuve d'une grande fiabilité d'un point de vue technique, la signature électronique qualifiée permettra au signataire qui y recourt de minimiser les risques inhérents

¹⁰⁰ Art. 28.3 et considérant n° 54 du Règlement eIDAS : les États membres sont toutefois libres d'intégrer des attributs spécifiques supplémentaires (comme un identifiant unique par exemple) à condition que ceux-ci ne soient pas obligatoires et qu'ils n'affectent en rien l'interopérabilité et la reconnaissance des signatures électroniques qualifiées.

¹⁰¹ Nous renvoyons à ce sujet à la contribution de H. Jacquemin dans le présent ouvrage.

¹⁰² D. MOUGENOT, « La preuve », *op. cit.*, p. 220.

¹⁰³ *Ibid.*, p. 222 ; D. GOBERT et E. MONTERO, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », coll. Cahiers du C.R.I.D., n° 17, Bruxelles, Bruylant, 2000, n° 56.

à l'usage de celle-ci. Trois avantages vont en effet de pair avec l'utilisation d'un tel procédé. Tout d'abord, une signature électronique qualifiée est assimilée de plein droit à une signature manuscrite comme nous l'avons vu. Le juge ne dispose d'aucun pouvoir d'appréciation à ce sujet. Dès lors, lorsqu'une signature manuscrite est requise par la loi, celle-ci pourra être remplacée par une signature qualifiée de manière tout à fait valable. Ensuite, en cas de contestation de la validité du procédé, l'utilisateur de la signature électronique qualifiée bénéficie d'un avantage en ce qui concerne la charge de la preuve, celle-ci étant beaucoup plus facile à rapporter. Enfin, une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres. Ce principe de reconnaissance mutuelle des signatures électroniques qualifiées au sein de l'Union européenne sera d'une grande utilité et facilitera la tâche des personnes ayant des activités dans différents pays de l'Union.

35.- Utilisation d'un pseudonyme. Tout comme la directive l'autorisait¹⁰⁴, le Règlement reconnaît au signataire la faculté de recourir à l'utilisation d'un pseudonyme. Toutefois, s'il est fait usage de cette faculté, cela doit être mentionné et le prestataire de service de confiance peut être tenu, à la requête des autorités, de fournir les données permettant d'identifier légalement la personne¹⁰⁵.

36.- Procédure de validation des signatures. En ce qui concerne la validation des signatures électroniques qualifiées, le considérant 57 prévoit que :

« Pour garantir la sécurité juridique concernant la validité de la signature, il est essentiel de préciser les éléments de la signature électronique qualifiée que devrait vérifier la partie utilisatrice effectuant la validation. En outre, le fait de définir les exigences applicables aux prestataires de services de confiance qualifiés qui peuvent fournir un service de validation qualifié aux parties utilisatrices ne voulant ou ne pouvant pas effectuer elles-mêmes la validation de signatures électroniques qualifiées devrait inciter les secteurs privé et public à investir dans de tels services. Les deux éléments devraient faire de la validation de signatures électroniques qualifiées une procédure aisée et adaptée à toutes les parties au niveau de l'Union ».

Le Règlement définit donc la validation comme étant « le processus de vérification et de confirmation de la validité d'une signature ou d'un

¹⁰⁴ Art. 8.3 de la directive 1999/93/CE.

¹⁰⁵ Considérant n° 33 et art. 32, e) du Règlement eIDAS.

cachet électronique »¹⁰⁶ et prescrit à l'article 32 les exigences applicables en la matière. À cet égard, le processus de validation d'une signature électronique qualifiée doit, pour confirmer la validité d'une telle signature, assurer que toutes les exigences requises pour qu'une signature électronique soit considérée comme qualifiée sont remplies. La validité d'une signature électronique qualifiée doit s'apprécier au moment où celle-ci est réalisée, et non au moment où le processus de validation prend place. Dès lors, une signature peut être parfaitement valide, même si le certificat a été révoqué, s'il est possible de démontrer que la révocation a eu lieu après le moment où la signature a été apposée¹⁰⁷.

Le système utilisé pour valider ce type de signature doit en outre fournir à la partie utilisatrice le résultat correct du processus de validation et lui permettre de détecter tout problème relatif à la sécurité¹⁰⁸.

Pour le surplus, la Commission européenne conserve, à l'instar de ce qui était prévu dans la directive, la faculté de prendre des actes d'exécution déterminant les numéros de référence des normes applicables aux services de validation qualifiés. Si le service respecte ces normes, il est présumé satisfaire aux exigences requises par le Règlement à l'article 33, § 1.

37.- Archivage des signatures électroniques qualifiées. Quant au service de conservation qualifié des signatures électroniques qualifiées, l'article 34 du Règlement précise qu'il doit être fourni par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures qualifiées au-delà de la période de validité technologique. En effet, il est important, d'un point de vue probatoire, d'être en mesure de démontrer, même des années plus tard, qu'un acte a bel et bien été signé. Prévoir la conservation à long terme des informations permet d'assurer la validité juridique des signatures électroniques sur de longues périodes de temps et de garantir qu'elles pourront être validées indépendamment de l'évolution technologique¹⁰⁹. Le Règlement a pris cette nécessité en compte en insérant cette disposition relative à l'archivage des signatures électroniques qualifiées.

§ 3. La signature électronique dans les services publics

38.- Reconnaissance mutuelle. Le Règlement contient une disposition spécifique relative à l'utilisation de la signature électronique dans les

¹⁰⁶ Art. 3.41 du Règlement eIDAS.

¹⁰⁷ P. LIPP, « Signature Validation – a Dark Art ? », in *Highlights for the Information Security Solutions Europe 2015*, Wiesbaden, Springer Vieweg, 2015, p. 198.

¹⁰⁸ Art. 32.2 du Règlement eIDAS.

¹⁰⁹ Considérant 61 du Règlement eIDAS.

services publics. Si un État exige qu'une signature électronique avancée soit utilisée pour avoir accès à un service offert en ligne par un organisme du secteur public ou en son nom, il doit reconnaître les signatures électroniques avancées, les signatures électroniques avancées qui reposent sur un certificat qualifié et les signatures électroniques qualifiées, ou d'autres formats validés conformément à des méthodes de référence spécifiques¹¹⁰. L'obligation de reconnaître des moyens d'identification électronique se rapporte donc uniquement aux moyens dont le niveau de garantie de l'identité correspond à un niveau égal ou supérieur au niveau requis pour le service en ligne en question¹¹¹.

Si l'on comprend aisément l'objectif de cette disposition, on s'interroge toutefois sur le deuxième type de signature auquel elle fait référence. Les signatures électroniques avancées qui reposent sur un certificat qualifié constituent-elles un quatrième type de signature consacré implicitement par le Règlement ? Un tel ajout pourrait s'expliquer par le fait que, dans certains États membres, des signatures avancées qui ne sont pas créées à l'aide d'un dispositif de création de signature électronique qualifié soient requises pour bénéficier des services d'un organisme public. La référence à ce type de signature peut être perçue comme étant le résultat d'un compromis trouvé entre les États afin de ne pas mettre à mal les systèmes et les infrastructures actuellement utilisés par différents pays.

Enfin, un État membre ne peut exiger que l'utilisation transfrontalière d'un service en ligne fournit par un organisme public soit conditionnée au recours à un procédé de signature électronique présentant des garanties de sécurité supérieures à celles de la signature électronique qualifiée¹¹².

§ 4. Les mesures transitoires propres aux signatures électroniques

39.- Période transitoire. Les personnes physiques ou morales qui utilisent des signatures électroniques reposant sur des certificats qualifiés devront veiller à ce que ceux-ci soient toujours valides et conformes au Règlement au 1^{er} juillet 2016.

¹¹⁰ Art. 27, 1 du Règlement eIDAS et Décision d'exécution 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du Règlement n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, J.O., L. 235 du 9 septembre 2015, pp. 37-41.

¹¹¹ Considérant 15 du Règlement eIDAS.

¹¹² Art. 27, § 3 du Règlement eIDAS.

Afin de garantir la sécurité juridique, l'article 51 du Règlement prévoit que les dispositifs sécurisés de création de signature conformes à la directive 1999/93/CE seront considérés comme des dispositifs de création de signature électronique qualifiés au sens du Règlement.

Par ailleurs, les certificats qualifiés dont disposaient les personnes physiques sous l'empire de la directive 1999/93/CE sont considérés comme des certificats qualifiés de signature électronique au sens du Règlement jusqu'à leur expiration. Les nouvelles cartes d'identité électronique belges, qui contiennent un certificat qualifié valable dix ans, resteront valables pendant cette période après l'entrée en vigueur du Règlement¹¹³.

Par contre, les personnes morales qui disposaient d'un certificat qualifié de signature électronique devront très certainement avoir recours à l'avenir au cachet électronique, étant donné que le législateur européen ne prévoit pas de mesure transitoire pour ces certificats¹¹⁴. Le silence du législateur à ce sujet laisse à penser que ces certificats perdront toute utilité dès l'entrée en vigueur du Règlement.

Les prestataires de services de certification qui délivraient jusqu'alors des certificats qualifiés au titre de la directive 1999/93/CE doivent soumettre un rapport d'évaluation de la conformité de leur service à l'organe de contrôle le plus rapidement possible, et au plus tard le 1^{er} juillet 2017. Jusqu'à l'achèvement de l'évaluation par l'organe de contrôle, ces prestataires de services de certification sont considérés comme des prestataires de services de confiance qualifiés au titre du Règlement eIDAS. En l'absence d'un tel rapport d'évaluation, ces prestataires de services de certification ne seront plus considérés comme des prestataires de services de confiance qualifiés à partir du 2 juillet 2017.

SECTION 2. – L'articulation du Règlement eIDAS avec l'article 1322, alinéa 2, du Code civil belge

40.- Articulation entre le droit européen et le droit national. Le nouveau cadre légal européen consacre trois catégories de signatures électroniques distinctes qu'il va falloir articuler avec l'article 1322, alinéa 2, du Code civil. En effet, si le législateur belge entend abroger la loi du 9 juillet 2001 dans le cadre de la mise en œuvre du Règlement, il n'entend toutefois pas en faire de même pour cette disposition du Code civil. Le

¹¹³ D. GOBERT, « Le Règlement européen du 23 juillet 2014 sur les services d'identification électronique et les services de confiance (eIDAS) : évolution ou révolution ? », *op. cit.*, p. 51

¹¹⁴ *Ibid.*

règlement eIDAS sera par ailleurs complété à l'avenir par une loi réglant, entre autres, certains aspects relatifs à la signature électronique¹¹⁵.

41.- En pratique à l'avenir. Le juge amené à trancher un litige portant sur une signature électronique devra examiner de quel type de signature il s'agit. S'il est confronté à une signature électronique qualifiée au sens du Règlement, celle-ci sera automatiquement assimilée à une signature manuscrite. Pour ce qui est des autres signatures électroniques, elles ne peuvent être privées d'effets juridiques au motif qu'elles se présentent sous forme électronique ou qu'elles ne sont pas qualifiées (principe de non-discrimination). La personne qui souhaite se prévaloir d'une signature électronique non-qualifiée devra pouvoir rapporter la preuve, en cas de contestation et dans le but d'emporter la conviction du juge, que sa signature remplit les fonctions qui lui sont reconnues en droit national¹¹⁶. En droit belge, nous avons vu que la doctrine reconnaît traditionnellement deux fonctions à la signature (identification du signataire et adhésion au contenu), mais que le législateur a rajouté, à l'article 1322, alinéa 2, du Code civil, une troisième exigence propre à l'environnement numérique : celle du maintien de l'intégrité du contenu de l'acte.

Selon la doctrine, lorsque l'on tombe sous le champ d'application de l'article 1322 du Code civil, cela a pour conséquence qu'une signature électronique ne permettant pas de garantir qu'un document n'a pas été modifié ne pourra se voir reconnaître les mêmes effets juridiques qu'une signature manuscrite en droit belge.

Néanmoins, et bien qu'il eût été préférable de conférer la fonction d'intégrité au support numérique et/ou aux processus techniques y afférents plutôt qu'à la signature électronique en elle-même, il faut reconnaître que ce qui importe en pratique c'est « la nécessité de préserver, en tout état de cause, l'intégrité d'un acte signé »¹¹⁷. En ce sens, dans la pratique, on constate que la vérification de la réalisation des fonctions de la signature

¹¹⁵ Avant-projet de loi mettant en œuvre et complétant le Règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, version du 11 décembre 2015, disponible sur <http://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2015&num=702>, consulté le 12 février 2016.

¹¹⁶ H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », *op. cit.*, p. 83.

¹¹⁷ M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, *op. cit.*, p. 591.

étant très technique, l'appréciation faite par les magistrats du procédé de signature reste assez pragmatique. Ont d'ailleurs déjà été reconnues comme des signatures satisfaisant au prescrit de l'article 1322, alinéa 2 du Code civil, des signatures scannées¹¹⁸ et des signatures apposées au bas d'un e-mail¹¹⁹. S'il n'est pas certain que de telles signatures suffisent effectivement en elles-mêmes à préserver l'intégrité du document, il ressort de certaines applications jurisprudentielles¹²⁰ que cette exigence peut être rencontrée grâce aux processus et procédés techniques attenants à l'apposition de la signature électronique.

SECTION 3. – L'avant-projet de loi belge visant à compléter le Règlement eIDAS

42.- Modification du cadre légal national. À l'heure d'écrire ces lignes, un avant-projet de loi mettant en œuvre et complétant le Règlement eIDAS a été approuvé par le Conseil des ministres¹²¹. Il vise à insérer un titre 2 intitulé « Certaines règles relatives au cadre juridique pour les services de confiance » au sein du livre XII du Code de droit économique. Le projet de loi a été soumis à la Commission européenne dans le cadre de la procédure obligatoire d'information¹²². Dans l'attente de l'avis de la Commission, le projet est bloqué jusqu'à la mi-mars 2016.

Si ce projet de loi a pour objectif principal d'instaurer un régime légal pour les prestataires de services d'archivage électronique, il contient néanmoins quelques dispositions en matière de signature électronique. Il a notamment vocation à insérer une présomption de validité de la signature

¹¹⁸ Conseil contentieux étrangers, 19 novembre 2009, n° 34364, www.rvv-ccf.be ; Conseil contentieux étrangers, 17 décembre 2009, *Rev. dr. étr.*, 2009.

¹¹⁹ Conseil de discipline des barreaux francophones du ressort de la cour d'appel de Bruxelles, 4 avril 2014, *J.L.M.B.*, 2014, pp. 937-941.

¹²⁰ Conseil contentieux étrangers, 19 novembre 2009, n° 34364, www.rvv-ccf.be.

¹²¹ Avant-projet de loi mettant en œuvre et complétant le Règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, version du 11 décembre 2015, disponible sur <http://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2015&num=702>, consulté le 12 février 2016.

¹²² Directive 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.*, L. 241 du 17 septembre 2015, pp. 1-15.

ture au profit de la partie qui utilise la signature électronique qualifiée. Ceci implique qu'avant de se fier à cette signature, la partie utilisatrice de la signature la vérifie au moyen d'un service de validation conforme aux articles 32 et 33 du Règlement¹²³.

En outre, le projet de loi va plus loin que le Règlement lorsqu'il prévoit que la signature électronique du titulaire de certificat peut être matérialisée par un équivalent satisfaisant aux exigences relatives à une signature électronique avancée. Le projet de loi reprend en fait le principe tel qu'il était déjà prévu à l'article 4, § 6, de la loi du 9 juillet 2001 et qui permet à un document électronique signé de ne pas perdre sa valeur lorsqu'il est imprimé, à condition que les exigences de la signature électronique avancée soient respectées. Cette disposition vise donc à permettre l'usage de la signature électronique dans un environnement hybride¹²⁴.

De plus, en son chapitre 5, le projet de loi énumère les hypothèses dans lesquelles un certificat qualifié de signature électronique doit être révoqué, suspendu ou arrivé à échéance.

Le Règlement abrogeant la directive 1999/93/CE, la loi du 9 juillet 2001 qui transpose cette directive doit, en toute logique, subir le même sort. C'est d'ailleurs ce que prévoit le projet de loi. Il reprendra pour partie les dispositions de la loi du 9 juillet 2001 et engendrera la modification de certains articles tels que la clause transversale générale figurant à l'article XII.15 du Code de droit économique¹²⁵.

Conclusion

43.- Application du Règlement. Au terme de notre analyse, il apparaît que le Règlement ne souffle mot des hypothèses dans lesquelles une signature serait requise juridiquement, question qui relève des prérogatives des États membres¹²⁶. Nous avons précédemment vu qu'une signature peut

¹²³ Art. XII.34 de l'avant-projet de loi mettant en œuvre et complétant le Règlement (UE) n° 910/2014.

¹²⁴ À ce sujet voy. J. VANDENDRIESSCHE, « Hybrid signatures under Belgian Law », *op. cit.*, pp. 79-80.

¹²⁵ Il faudra à l'avenir la lire comme suit « Toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées. L'exigence, expresse ou tacite, d'une signature est satisfaite dans les conditions prévues soit à l'article 1322, alinéa 2, du Code civil, soit à l'article 3.12 du Règlement 910/2014 (signature électronique qualifiée) ».

¹²⁶ D. GOBERT, « Le Règlement européen du 23 juillet 2014 sur les services d'identification électronique et les services de confiance (eIDAS) : évolution ou révolution ? », *op. cit.*, p. 31.

être utile à des fins probatoires, mais aussi être une condition nécessaire à la validité d'un acte juridique. Le Règlement trouve à s'appliquer dans les deux hypothèses, que la signature soit requise *ad probationem* ou *ad validitatem*.

44.- Analyse de risques. D'un point de vue probatoire, si les effets juridiques d'une signature électronique qualifiée sont assurés, il n'en est pas de même pour les autres types de signatures électroniques. Une incertitude subsiste quant à l'appréciation que feront les magistrats de la valeur probante qu'il convient de reconnaître à une signature électronique ordinaire ou avancée en justice. Dès lors, il faut être conscient qu'opter pour l'usage d'une signature électronique ordinaire ou avancée ne permet pas de s'assurer des effets juridiques qui y seront attachés par la suite en cas de contestation. Si l'on recherche un degré élevé de sécurité juridique, il vaut mieux s'orienter vers l'utilisation de la signature électronique qualifiée étant donné le régime de faveur que le Règlement lui réserve.

45.- Harmonisation partielle. *In fine*, si, pour les autres services de confiance, le Règlement eIDAS s'attèle à définir les fonctions de chacun d'eux, tel n'est pas le cas pour la signature électronique. Cette manière de procéder a pour effet de laisser subsister le doute en matière de signature électronique. Alors que le Règlement a pour objectif de simplifier les règles applicables aux services de confiance afin d'instaurer un climat de confiance dans l'environnement en ligne, la clarification opérée au niveau européen en matière de signature électronique apparaît comme entachée d'une incertitude. En laissant à chaque État membre le pouvoir de déterminer ce qu'il convient d'entendre par « signer », le législateur ouvre la porte aux interprétations divergentes. En effet, les fonctions de la signature étant le socle de tout le régime juridique relatif à la signature électronique mis en place par le Règlement eIDAS, des différences majeures pourraient exister au sein de l'Union et mettre en péril la sécurité juridique que les utilisateurs des services de confiance sont en droit d'attendre.

Toutefois, la marge de manœuvre laissée aux États membres à cet égard trouve très certainement sa raison d'être dans l'absence de volonté de ceux-ci de procéder à une harmonisation plus poussée de leurs droits nationaux. Dès lors, le Règlement a pour mérite, en matière de signature électronique, de clarifier les concepts qui régissent la matière et d'insuffler un nouveau souffle à l'utilisation de la signature dans l'environnement numérique. Il reste à espérer qu'en pratique le recours aux signatures électroniques se fera de manière plus aisée et systématique à l'avenir afin d'accroître la sécurité juridique et d'accélérer les transactions dans l'environnement virtuel.